

Demonstration of an Active Quantum Key Distribution Network¹

Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang,
David Su, Ronald F. Boisvert, Charles Clark, and Carl Williams

National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899
xiao.tang@nist.gov; alan.mink@nist.gov

ABSTRACT

We previously demonstrated a high speed, point to point, quantum key distribution (QKD) system with polarization coding over a fiber link, in which the resulting cryptographic keys were used for one-time pad encryption of real time video signals. In this work, we extend the technology to a three-node active QKD network - one Alice and two Bobs. A QKD network allows multiple users to generate and share secure quantum keys. In comparison with a passive QKD network, nodes in an active network can actively select a destination as a communication partner and therefore, its sifted-key rate can remain at a speed almost as high as that in the point-to-point QKD. We demonstrate our three-node QKD network in the context of a QKD secured real-time video surveillance system. In principle, the technologies for the three-node network are extendable to multi-node networks easily. In this paper, we report our experiments, including the techniques for timing alignment and polarization recovery during switching, and discuss the network architecture and its expandability to multi-node networks.

Keywords: Quantum cryptography, quantum key distribution, quantum communications network, optical switches.

1. INTRODUCTION

Since Quantum Key Distribution (QKD) was first proposed in 1984 [1], many groups have implemented and demonstrated QKD systems. A variety of these efforts were reported in the comprehensive review article [2]. In recent years tremendous efforts have been focused on increasing both the distance between communicating parties as well as the speed in which cryptographic keys can be established. Most QKD systems reported have been point-to-point links. Only a few groups, such as BBN [3], have demonstrated quantum networks with three nodes or more.

Phoenix et al. [4] proposed the concept of passive quantum networks using passive optical components. Such a network adopts passive optical couplers as network nodes to split photons sent by Alice, the transmitter, to more than one Bob, the receiver. In this architecture, simultaneous communication, or “broadcast”, from one user to all others in the network is established and quantum key distribution between one user to any other one can be realized. Townsend et al. [5] conceptually demonstrated that quantum key distribution is feasible between any user to any other one within a passive quantum network. However, in the passive communication network, photons (and hence the bit that it represents) are split by couplers according to their ratio and hence only a subset of these photons reach each terminal node. So, the actual key rate between specific terminals is greatly reduced. In comparison, in an active QKD network a network controller actively controls optical switches to direct the communication direction (orientation). In this case, all photons emitted by Alice (except those lost in the link) are delivered to the selected terminal yielding the full communication speed (therefore highest quantum key rate) between two users in the network.

In this work, we demonstrate a high-speed three-node active QKD network with one Alice and two Bobs each connected to Alice by 1 km fiber links. Two optical switches are actively controlled to alter the connection between Alice and each

¹ The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.

Report Documentation Page			<i>Form Approved OMB No. 0704-0188</i>					
<p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>								
1. REPORT DATE AUG 2006	2. REPORT TYPE	3. DATES COVERED 00-00-2006 to 00-00-2006						
4. TITLE AND SUBTITLE Demonstration of an Active Quantum Key Distribution Network			5a. CONTRACT NUMBER					
			5b. GRANT NUMBER					
			5c. PROGRAM ELEMENT NUMBER					
6. AUTHOR(S)			5d. PROJECT NUMBER					
			5e. TASK NUMBER					
			5f. WORK UNIT NUMBER					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Institute of Standards and Technology,100 Bureau Drive,Gaithersburg,MD,20899			8. PERFORMING ORGANIZATION REPORT NUMBER					
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)					
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)					
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited								
13. SUPPLEMENTARY NOTES Proc. SPIE Vol. 6305, 630506 (August 2006)								
14. ABSTRACT see report								
15. SUBJECT TERMS								
16. SECURITY CLASSIFICATION OF: <table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="padding: 2px;">a. REPORT unclassified</td> <td style="padding: 2px;">b. ABSTRACT unclassified</td> <td style="padding: 2px;">c. THIS PAGE unclassified</td> </tr> </table>			a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 6	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified						

of the Bobs. Over 1 Mbps sifted-key rate is generated in either link. Based on this architecture we discuss feasible schemes for one-to-any and any-to-any active quantum networks as well as their potential applications.

2. SYSTEM CONFIGURATION

We previously reported [6-8] point-to-point polarization encoding QKD systems with protocols of both B92 [9] and BB84 [1] operated over 1 km of optical fiber. These QKD systems used 850 nm photons in the quantum channels to match the detection range of silicon avalanche photo diode (APD), and telecom wavelengths (1510 nm and 1590 nm) in the bi-directional classical channels. The systems were synchronized at a clock rate of 1.25 Gbit/s, with a quantum channel transmission rate (QCTR) as high as 625 MHz (2 clock periods).

Based on our previous work we have demonstrated an active three-node QKD network as shown schematically in Fig. 1. Two MEMS optical switches are installed at the Alice side: one at 1550 nm band to redirect the classical channels; the other at 850 nm band for the quantum channels. The optical switches can be controlled manually or by a computer. There are two fibers connecting Alice and Bob1: one is an 850 single mode fiber (HI780, 1 km) for the quantum channel and the other is a standard telecom fiber (SMF28, 1 km) for the classical channel. There are two standard telecom fibers (SMF28, 1 km for each) used to connect Alice and Bob2: one for the classical channel and the other for the quantum channel. A short piece (~ 20 cm) of HI780 fiber is fusion spliced at the end of the SMF28 fiber for the quantum channel. This short piece of HI780 fiber functions as a spatial filter to remove 850 nm higher mode components generated in the 1550 nm fiber. Two different types of programmable polarization controllers (liquid crystal type at Bob 1 and piezo type at Bob 2) are installed to recover and automatically compensate for polarization evolution caused during transmission in the fiber loops.

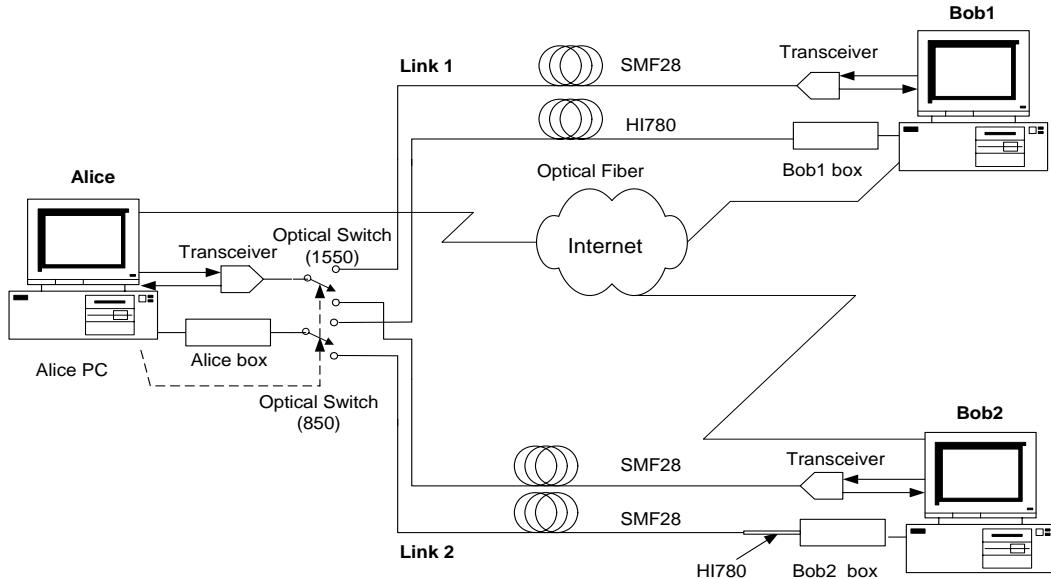


Figure 1. Configuration of active three-node QKD secured network

High-speed data handling boards, designed and implemented at NIST, are installed at both Alice and Bobs' computers. The board at Alice generates pseudo-random data streams to fire corresponding lasers in accordance with the QKD protocol. The photons from the suitably attenuated lasers are then directed by an optical switch to one of the two optical paths (Link1 and Link2) and the respective Bob at the end of the path. The board at each Bob collects the detection events and communicates with Alice via a classical channel to perform the sifting algorithm. Alice and Bob's boards then send the sifted bit values to their own computers for subsequent error reconciliation and privacy amplification performed over the classical channel necessary to generate shared secret keys [10-11]. The computers of Alice and Bob

then use the shared secret keys for application-level data encryption necessary to implement secured communications through an unsecured network.

The system can perform either BB84 or B92 protocol by a straightforward altering of the Alice and Bob boxes. In this work, we use the B92 protocol for a demonstration.

3. RESULTS AND DISCUSSION

In this experiment we use two optical switches to select a communication destination from Alice to Bob1 or Bob2. As long as Alice and one of the two Bobs are connected, the point-to-point protocol can be readily applied to the link and quantum keys are generated and shared by the two terminals. Therefore, the sifted-key rate and quantum bit error rate (QBER) used to characterize performance for each link are the same as for previously demonstrated point-to-point communications. However, the time to establish the initial connection between Alice and one of the Bobs, as well as the time needed to switch the connection from one Bob to another, are also important parameters to characterize the performance of the three-node network. We measured these parameters in the experiment.

The sifted-key rate R in each link of the QKD network can be estimated by the following equation when the influence of the APD's dead time is ignored. (The sifted-key rate estimation equation considering APD's dead time has been discussed elsewhere [12])

$$R = \mu \cdot L_{sw} \cdot L_f \cdot L_o \cdot Pd \cdot L_p \cdot \nu \quad (1)$$

Here the mean photon number μ is set to 0.1. L_{sw} is the loss in optical switches, which is about 0.8 dB in our system. L_f is the loss in the transmission fiber, which is measured to be 2.3 dB/km at 850 nm for the fibers (SMF 28 and HI780) used in the two links. L_o represents other losses such as bending, coupling and connection losses in the quantum channel, which is about 3 dB in our case. Pd is the APD's detection efficiency, about 45% (3.5 dB) at 850 nm according to the manufacturer's specification. L_p is the protocol related loss, which is 3 dB for BB84 since half of the counts are discarded in the protocol and 6 dB for B92 since all incompatible photons and half of the compatible photons are blocked before entering the detector. ν denotes the quantum channel transmission rate (QCTR). In our experiment we use a QCTR of 625.0 Mbit/s, which corresponds to Alice generating one optical pulse in every 2 clock periods. The measured sifted-key rates in the two links are 1.71 Mbps and 1.55 Mbps, respectively, which is in good agreement with the value estimated by Eq. (1). Since standard telecom fiber is used in the second link, some photons emitted by Alice are shifted from the fundamental mode into a higher-order mode during transmission and subsequently filtered at the end of the link. That causes a lower sifted-key rate in the second link than that of the first. In comparison with our point-to-point QKD system, the sifted-key rate in the network is approximately 0.8 dB lower due to loss resulting from the insertion of optical switches.

For a point-to point QKD system, the QBER is mainly due to polarization leakage or imperfect extinction ratio, timing jitter, data-dependant jitter and dark counts as discussed in [8]. In this work, the QBER measured in the first and second links are 2.9% and 3.3%, respectively. Although the most of the high-order mode photons are filtered by the sliced HI780 fiber, the presence of these photons contributes to the slightly higher QBER in the second link. Nevertheless, the values of QBER measured in both links are very close to the QBER in our point-to-point QKD system, which indicates that the optical switches are stable and do not contribute significantly more errors to the links in the QKD network system.

In an active QKD network, we define a connection time, which is time between when the optical switch receives the switch signal for connecting a link to when the link can generate secret keys. The connection time is an important metric for active networks. After switching, Alice and the Bob need to do polarization recovery and software initialization before the two terminals can generate secret keys. The connection time T_{ct} consists of the following three parts:

$$T_{ct} = T_{sw} + T_{pr} + T_{si} \quad (2)$$

Here T_{sw} is the switching time of the optical switch, which is less than 1 ms in our case. T_{pr} is the time for performing polarization recovery. In our system, the time for polarization recovery is relatively long, which are 360 sec and 480 sec for Link 1 and Link 2, respectively. In Link 1 we used a liquid crystal type of polarization controller that has a relatively long response time. In Link 2 we used a piezo type of polarization controller. Although the latter's response time is much faster, its interface communication speed with the PC is slow. T_{si} is the software initialization time, which includes raw key sifting, error reconciliation, privacy amplification and initial key buffering. T_{si} depends on the speed of both Alice and Bob's computers as well as the key rate. In this experiment, it is about 60-120 sec. So, polarization recovery is the most time-consuming process in connection. We are currently undertaking research in order to reduce polarization recovery time [13].

4. ACTIVE QKD NETWORK AND ITS POTENTIAL APPLICATIONS

The architecture of our three-node QKD network can be extended to one-to-any and any-to-any communication within the network. The one-to-any structure (one Alice to many Bobs) is shown in Fig. 2(a). Optical switches control the communication destinations. The one-to-any structure is natural extension of our three-node architecture obtained by replacing the 1×2 optical switch with $1 \times n$ optical switch. The system configuration and system performance, such as sifted-key rate, QBER and connection time, would be similar to the experimental system described above. The general structure can also implement quantum key distribution between many Alices and one Bob. For an any-to-any architecture, optical cross connect (OXC) switches are used to implement communications between any Alice and any Bob as shown in Fig. 2(b). It has been reported [14] that some advanced OXCs, such as MEMS devices have been constructed to support 1024×1024 optical channels, which paves the way to implementing any-to-any network based on this architecture. One new issue in any-to-any networks is that a Bob may communicate with many Alices that may be at a different distances, requiring Bob to conduct a time alignment procedure after each switching operation, thus adding to the connection time. We have developed automatic time-alignment software to implement a fast time alignment.

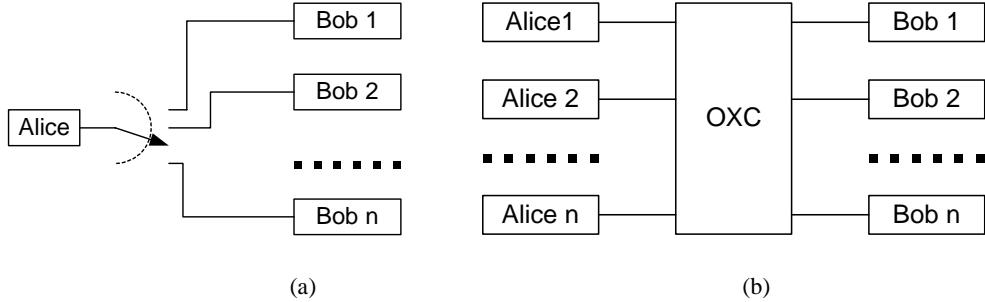


Figure 2. Multiple user architecture for active QKD networks: (a) one-to-any network, and (b) any-to-any network.

The active QKD network topology can be a branch configuration or a loop configuration as shown in Fig. 3. In a branch configuration, a provider is one or many Alices, and every node is an optical switch or an OXC to direct the connection orientation to certain users (Bobs). In a loop configuration, a provider (one or many Alices) provides an information loop, and users (Bobs) can access the loop by optical switches or OXC. Whether in branch or loop configuration, any user can implement communication with a certain Alice in the providers after the optical switches or OXC are correctly set.

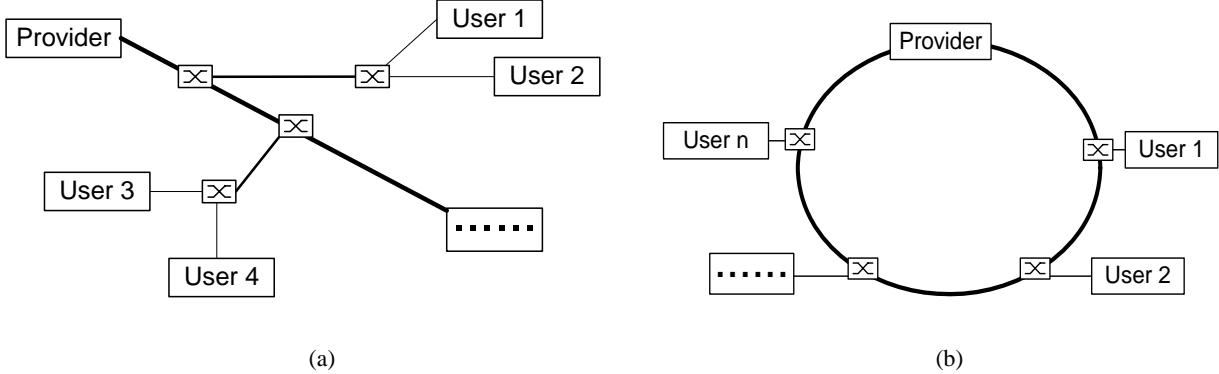


Figure 3. Potential topography of active QKD networks: (a) a branch-configuration, and (b) a loop-configuration.

In any active QKD network, whether one-to-any or any-to-any, or branch configuration or loop configuration, a QKD network management system is needed. The management system responds to requests of terminals of the network, and sets optical switches or the OXC to establish the corresponding connection in the network.

The above mentioned one-to-any and any-to-any structures can implement quantum key distribution between one Alice to one of many Bobs (or one of many Alices to one Bob) and one of many Alices to one of many Bobs. However, it can not implement simultaneous quantum key distribution between two Alices or two Bobs. In order to implement quantum key distribution between any two network nodes, a full-function QKD terminal, or duplex QKD terminal, which has both Alice and Bob functions, must be available at each node in the network. In some specific applications, however, some nodes in a network need not communicate between each other, and hence a one-function QKD terminal, or simplex QKD terminal (Alice or Bob), can be used to reduce cost.

As described above, an active QKD network can generate secure keys without any significant degradation compared to a point-to-point system. For such a network, a wide range of potential applications can be realized in Local Area Networks (LAN). One example of an important and feasible applications is a QKD secured video surveillance network, in which a one-to-any network structure is used as shown in Fig. 4. Each Bob at different locations is equipped with a monitoring video camera, while Alice is installed at surveillance station. Alice can control the optical switches to connect to any Bob terminal and initiate quantum key distribution. Once the secret quantum keys are generated and shared between Alice and Bob, the video content taken by the monitoring camera at the Bob can be encrypted using the secret key bits and sent to Alice over an unsecured public network, such as the Internet. Alice can then decrypt the transmitted data to view the video. The speed of our system enables the real-time key exchange sufficient to support one-time pad encryption/decryption of streaming video. We are developing such a two-camera surveillance system based on the three-node QKD network.

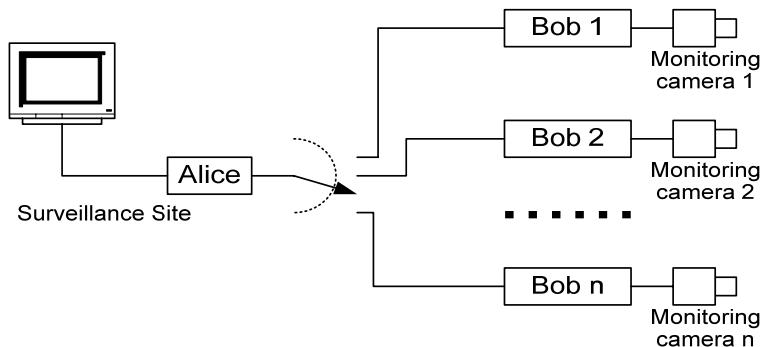


Figure 4. QKD secured network application: secured surveillance system.

5. CONCLUSION

We have demonstrated an active three-node QKD network, which generates sifted-key at a rate over 1 Mbps between terminals. Two optical switches actively control its communication orientation. This network architecture can be extended to allow one-to-any and any-to-any quantum key distribution in optical networks. As an example of its potential applications, a QKD secured surveillance network is also discussed.

ACKNOWLEDGEMENT

This work was supported in part by the Defense Advanced Research Projects Agency under the DARPA QuIST program.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing" in Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing, pp. 175-179, Bangalore, India, December 10-12, (1984).
2. N. Gisin G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74, 145-195 (2002).
3. Chip Elliott, "Building the quantum network", New Journal of Physics, Vol. 4, page 46.1-46.12 (2002).
4. S. Phoenix, S. Barnett, P. Townsend, and K. Blow, "Multi-user quantum cryptography on optical networks", Journal of Modern Optics, 72 (6): 1155-1163 (1995).
5. P. Townsend, S. Phonenix, K. Blow, and S. Barnett, "Design of quantum cryptography systems for passive optical networks", Electronics Letters, 30(22), 1875-1877 (1994).
6. Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Barry Hershman, Joshua Bienfang, Ronald F. Boisvert, Charles Clark, and Carl Williams, "High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding," in Optics and Photonics 2005: Quantum Communications and Quantum Imaging III, Proc. SPIE 5893, 1A-1-1A-9 (2005).
7. Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang, David Su, Ronald F. Boisvert, Charles Clark, and Carl Williams, "Quantum Key Distribution system operating at sifted key-rate over 4 Mbit/s", Defense and Security 06, Proc. SPIE 6244, 62440P-1~62440P-8 (2006).
8. Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua Bienfang, David Su, Ronald F. Boisvert, Charles Clark, and Carl Williams, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s", Optics Express, Vol. 14 (6): 2062-2070 (2006).
9. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., 68, 3121-3124 (1992)
10. A. Nakassis, J. Bienfang, and C. Williams, "Expeditious reconciliation for practical quantum key distribution," in Defense and Security Symposium: Quantum Information and Computation II, Proc. SPIE 5436, 28-35 (2004)
11. Alan Mink, Xiao Tang, Lijun Ma, Tassos Nakassis, Barry Hershman, Joshua C. Bienfang, David Su, Ron Boisvert, Charles W. Clark, and Carl J. Williams, "High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video", Defense and Security 06, Proc. SPIE 6244, 62440M-1~62440M-7 (2006)
12. Hai Xu, Lijun Ma, Joshua Bienfang, and Xiao Tang, "Influence of the dead time of avalanche photodiode on high-speed quantum-key distribution system", CLEO/QELS 2006, CLEO digest JTuH3, May 2006.
13. Lijun Ma, Hai Xu and Xiao Tang, "Polarization recovery and auto-compensation," in Optics and Photonics 2006, San Diego, Aug.13~17.
14. T. Bifano, "Optical Cross Connect Switches for Communication Network", <http://mle2.bu.edu/mn500/pdf/Class7&8.pdf>